

5/5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067544 A2

(51) International Patent Classification⁷: **H04L 29/06**

(21) International Application Number: PCT/US02/04641

(22) International Filing Date: 15 February 2002 (15.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/269,699 17 February 2001 (17.02.2001) US

(71) Applicant: **INKTOMI CORPORATION** [US/US]; 4100
East Third Avenue, Foster City, CA 94404 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

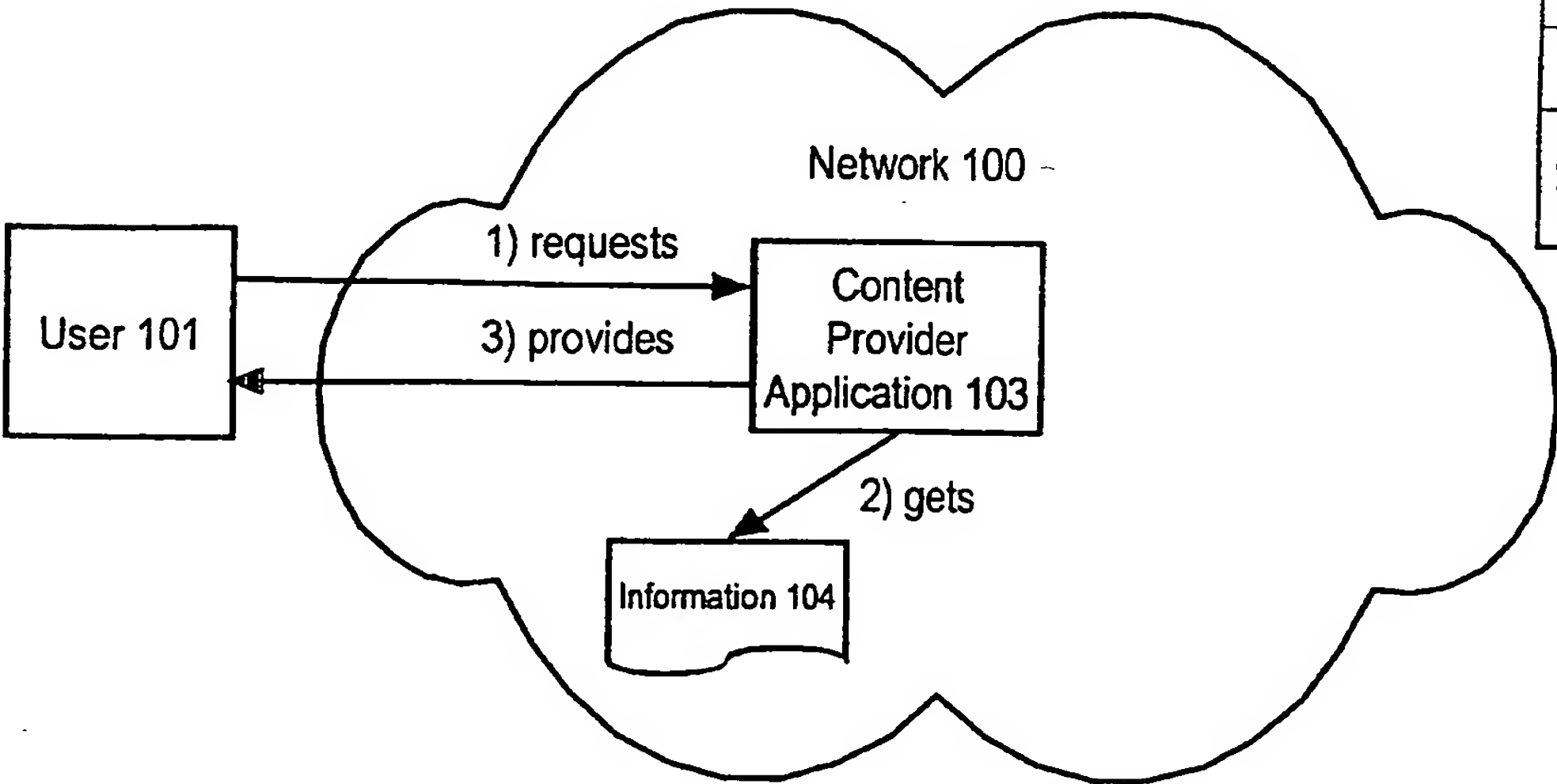
Published:
— without international search report and to be republished upon receipt of that report

(72) Inventor: **TSO, Michael**; 20555 Ashley Way, Saratoga, CA 95070 (US).

(74) Agents: **EICHSTAEDT, Cheryl et al.**; Hickman Palermo Truong & Becker, LLP, 1600 Willow Street, San Jose, CA 95125 (US).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **HEADER-BASED NETWORK API**



FP03-0201
- 00EP-NT
04. 4.-1
SEARCH REPORT

(57) Abstract: A method and apparatus for communicating with entities outside of a secure network by intercepting and modifying messages is provided. Techniques for accomplishing the communication include inserting, retrieving, and deleting information from messages. The entities involved in the communication include, but are not limited to, users, content providers, and access providers. Furthermore, the types of information used in modifying messages include billing, location, demographic information, profile data, multimedia data, and code.

WO 02/067544 A2

HEADER-BASED NETWORK API

PRIORITY CLAIM AND CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to and claims domestic priority from prior U.S. Provisional Application Serial Number 60/269,699, filed on February 17, 2001 entitled "Content-Based Billing and Header Based Network API", by Michael M. Tso, Pei-Yuan Zhou, Ivry Semel, Sailendrak Padala, and Philippe Le Rohelec, the entire disclosure of which is hereby incorporated by reference as if fully set forth herein.

FIELD OF THE INVENTION

The present invention relates to network communications, and more specifically, to using an intermediary to intercept and modify messages between participants.

BACKGROUND OF THE INVENTION

The Internet is a network composed of many smaller private networks. Frequently, parties that are outside a particular private network would like to have access to information maintained securely within that particular private network. For example, content providers would often like to access information possessed by access providers. The information maintained by an access provider to which content providers may want access may include, for example, the current location of a mobile device user, the billing information of a user, demographic information about the user, etc. In general, this information is maintained secure within the access provider's private network.

There are two general approaches for making information maintained securely within a private network available to third parties that are authorized to use it. The first approach is to execute the third party's application within the private network. For example, an access provider could host, within access provider's own network, the applications of content providers (hereinafter referred to as "content provider applications").

Figure 1 shows a system in which a content provider application 103 is executed within the private network 100, which is a secure network containing information the access provider controls. Referring to Figure 1, the user 101 requests information 104 from content provider application 103. To satisfy user 101's request, the content provider application 103 retrieves information 104 where the content provider application 103 and the information 104 reside inside the secure network 100. Then the content provider application 103 provides the requested information 104 to user 101.

The approach of hosting the content provider applications within the private network of the access provider does not scale well, since the more third party applications that the access provider executes within its network, the greater the likelihood that the applications will conflict with each other, or with other programs within the access provider's network. The overall reliability and integrity of the network is affected as a result.

The second approach is for the access provider to provide each content server with a mechanism, such as a program (hereinafter referred to as "access provider program"), an encryption key, or encryption password that enables each content server to access the appropriate information using often proprietary interfaces as well as traversing through the access provider's firewall. Figure 2 is a block diagram of a system in which a user 201 requests content from a content provider, which the content provider application 203 is associated with. As a result of the user 201's request, the content provider application 203 accesses information 204 from network 200, which is a secure network containing information the access provider controls, using an access provider program 205. The content provider application 203 requests information 204 from the access provider program 205. The access provider program 205 retrieves the information 204 from inside the secure network 200. Then the access provider program 205 provides the retrieved information 204 to the content provider application 203. Then the content provider application 203 provides the information 204 to user 201.

The approach of providing access provider programs to content providers is undesirable due to the security threat raised by providing a tunnel through the firewall's security. Malicious parties could study how the access provider software is getting around the firewall, and create their own programs to do the same. There is also a problem with supporting and maintaining a piece of code distributed to potentially thousands of content providers. The proprietary interfaces to the private network's systems may change over time which would require updating and integration testing of the access provider software.

Another negative aspect of accessing information in a secure network associated with an access provider either with an access provider program or a content provider application is the time that is required for a content provider to prepare a legal contract (e.g., "commercial terms of agreement") when offering a new service. As a part of this contractual agreement, the access provider needs to maintain and check a database of pre-configured entries for each content provider that the access provider is associated with.

Based on the foregoing, it is clearly desirable to provide techniques that allow

authorized third parties to access confidential data maintained by within a private network, without threatening the security of the data, nor requiring the controller of that network to host third party applications.

SUMMARY OF THE INVENTION

Techniques are provided for communicating with entities outside of a secure network by using an intermediary to intercept, modify, and forward messages that are being sent to those entities. The intermediary intercepts the messages and may insert, retrieve, and/or delete information from messages. According to one aspect of the invention, the modifications are made in such a way that a recipient that is not expecting the modifications made by the intermediary will still successfully receive the information from the original message. For example, in one embodiment, the intermediary inserts the information into the headers of the messages in a way that will be ignored by recipients that are not expecting the information.

The entities involved in the communication may include but are not limited to users, content providers, and access providers. The types of information that the intermediary adds to the intercepted messages will vary from implementation to implementation, and may include billing, location, demographic information, profile data, multimedia data, and software programs.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Figure 1 is a block diagram of a system in which an access provider hosts content provider applications;

Figure 2 is a block diagram of a system in which an access provider provides a program by which content providers can access information maintained by the access provider;

Figure 3 is a block diagram of a system in which an access provider intercepts a user's request and piggybacks information for the content provider on the message containing the user's request, according to an embodiment of the invention;

Figure 4 is a block diagram of a system in which information from within a network is provided to parties outside the network using the headers of messages that are being sent to those parties, according to an embodiment of the invention;

Figure 5 is a block diagram of the content provider piggybacking information on a message containing a response to a user request, according to an embodiment of the invention;

Figure 6a and 6b are block diagrams that illustrate a piggybacked conversation in detail;

Figure 7 is a block diagram that illustrates a piggybacked conversation where the access provider checks the content provider's profile, according to an embodiment of the invention; and

Figure 8 is a block diagram of a computer system on which embodiments of the invention may be implemented.

DETAILED DESCRIPTION OF THE INVENTION

A method and apparatus are described for communicating with entities outside of a secure network by intercepting and modifying messages. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

CONCERNING NOTATION IN THE FIGURES

As access providers, content providers, and users communicate information between each other, data is copied. As a matter of notation in the figures, the first copy of data will be indicated with a prime symbol and a second copy will be indicated with a double prime symbol. For example, if the original copy of data is indicated with the letter A, then the first copy of A will be A', and the second copy of A will be A''.

FUNCTIONAL OVERVIEW

Most network communications protocols use messages that have headers. Typically, a message header has information necessary to make sure the message is delivered to the correct destination. It may also include optional information, such as data that identifies the source of the message.

According to one aspect of the invention, information from a private network is conveyed to authorized parties outside the network by inserting the information into the header of messages that are directed to those parties, using optional fields in the header so

as to ensure correct delivery and handling of the message by intermediaries or destinations which may not be able to decode the information that has been inserted into the optional fields.

Specifically, HTTP is the protocol used for most Internet application traffic. The HTTP protocol specifies the transmission of information in blocks that have headers. According to one embodiment as depicted in Figure 3, when a user 301 sends a message 305 to a content provider application 303, the message 305 is intercepted by the proxy server 302 and, depending on the destination of the message 305, information 304 that is otherwise only available within the private network 300 of the proxy server 302 is inserted into the HTTP header of the message 305. Information 304 becomes information' when inserted into the HTTP header of message 305. Message 305 and information' become message 306 and information'' when transmitted over the network. The content provider application 303 retrieves the information'' from the header of message 306 when the content server receives the message 306.

Although figure 3 depicts the network intermediary as a proxy server, any network intermediary capable of intercepting and augmenting messages reliably, such as routers, switches, and load balancers, may be used. Furthermore, HTTP is not the only protocol that may be used. Therefore, any email protocol and packet data may be used, in which case the message body would be the data payload.

According to one embodiment, the information that the access server inserts into the message header relates to the user sending the message. For example, the information may indicate the current location of the user of a mobile device, or information from the user profile of the user.

The HTTP protocol allows optional application defined fields to be added to the header. Furthermore the HTTP protocol defines that intermediaries and destinations may simply pass any header fields that the intermediaries or destinations cannot comprehend without affecting the integrity of the data or the connection. If a protocol other than HTTP is used, and that other protocol does not support optional application defined fields, then a tunnel must be established between the access provider and the content provider. The tunnel will ensure that the intermediaries (such as routers and proxies) between the access provider and the content provider will correctly deliver the original message as well as the new data fields that have been inserted. Tunneling data by encapsulating one data format, for example with optional fields, in another data format is well known to those skilled in network protocol design.

PROVIDING INFORMATION FROM A PRIVATE NETWORK

Figure 4 is a block diagram of a system in which information from within a network is provided to parties outside the network using the headers of messages that are being sent to those parties. Referring to Figure 4, a user 401 accesses content and services from content servers (407a, 407b, 407c) through a proxy server 402 on a network 400a controlled by an access provider.

Various items of information are maintained within that network 400a, including location data 405, billing data 403, user profiles 406, and content provider profiles 404. Since information such as 403, 404, 405, and 406 are maintained inside network 400a, which is associated with an access provider, networks 400b and 400c do not have access to information 403, 404, 405 and 406. Some of the services from the content servers (407a, 407b, 407c) that are external to network 400a may desire access to some of that information. For example, a restaurant locator site, which is associated with content servers such as 407a, 407b, and 407c, may want access to a user's location data 405 in order to determine the closest restaurants to the user 401's location.

As another example, a content provider that charges a per-access fee may desire access to the billing data so that the content provider can post charges in the billing data that will be billed on the invoices generated by the access provider. This avoids the need for the content provider to send out its own bills, and would be particularly useful when the amount billed by the content provider is low relative to the cost of preparing a bill. A typical scenario could proceed as follows:

The proxy server intercepts a user request for a service associated with a URL. The proxy server inspects content provider profiles to determine the needs of the content provider/service associated with that URL. The destination address of the URL is used to identify the content provider.

The proxy server determines that the requested service requires the user's current location information.

The proxy server obtains the user's current location data and inserts the location data into the header of the intercepted request.

The proxy server then transmits the modified request to the content provider.

PROVIDING INFORMATION TO A PRIVATE NETWORK

Just as message headers may be used to carry data out of a private network, they may be used by third parties to provide data to a private network. For example, assume that a particular content provider charges different fees for accessing different content on its service. If the fee schedule for the particular content provider is maintained in a content provider profile within the private network, then the content provider profile for the content provider that is maintained by every access server has to be updated every time the fees change. On the other hand, the content provider may simply dynamically insert the current fee for accessing particular content into the message header of a message that delivers that particular content.

For example, assume that a content provider charges 5 cents for each stock quote, and the charge is to be billed by the access provider. Rather than maintain data indicating the 5 cent fee in the content provider profile, the content server may insert the fee amount in the header of each message that delivers a stock quote. Consequently, if the content provider decides to increase the fee to 7 cents, the content provider merely changes the data that determines the value inserted into the header. The access provider need not make any change to the content provider profile. Another example of when the header based network API would be advantageous is when there is a large number of items with different prices (such as software programs for downloading, grocery items, etc.). Maintaining a large number of items at the access provider would be a big task since maintaining these items entails updating the prices of the items as the prices fluctuate.

A typical scenario could proceed as follows:

The proxy server intercepts a request for a service provided by a content provider.

The request is forwarded to the content provider.

The content provider replies with a message that, within its header, indicates a particular fee for the service.

The proxy server intercepts the reply from the content provider.

The proxy server verifies that the content provider is an approved partner.

The proxy server checks the user profile to determine whether the user has sufficient funds, and whether the user is authorized to make such purchases.

The proxy server sends a message to the user requesting authorization of payment. Payment authorization may be bypassed if the user so indicates.

The proxy server receives authorization of payment from user.

The proxy server deducts the fee from the user's balance and forwards the content to the user.

SECURITY ISSUES

Under various circumstances, such as when a user is charged a fee from a third party, it is critical to authenticate the identity of the parties involved. The user is typically authenticated at the time the user starts a session by requiring the user to login with a valid user ID/password combination.

The third-party content provider may be authenticated, in turn, prior to completion of the transaction. For example, when the proxy server intercepts a request for a service, the proxy server may inspect the content provider profile to determine whether the service involves a fee. If it does, the proxy server may establish a secure connection with the content provider, and authenticate the content provider through any number of authentication mechanisms, such as through the use of digital certificates.

PIGGYBACKED CONVERSATION

As explained above, access providers can communicate information to content servers by inserting information into the header of messages, initiated by users, that are destined for the content servers as is depicted in figure 3. Likewise, content providers can communicate information to access providers by inserting information into the header of responses to those messages. Thus, by inserting data into message headers, an access provider and a content provider can effectively carry on a conversation that is piggybacked on the messages of users that are accessing the services of the content provider. Within such piggybacked conversations, the parties to the piggybacked conversation can authenticate each other, request information and respond to requests.

For example, assume that the access provider receives from a user a request for a service that is provided by a content provider about which it has no information. The access provider may simply forward the request to the content provider without inserting any information. The content provider may insert into the message header of the reply a request for location information.

When the access provider intercepts the message from the content provider, the access provider sees the request for location information. Rather than deliver the reply to the user, the proxy server may send a new request to the content server, where the header of the new request includes location information. The content server then responds with content that is based upon the location information, which the proxy server sends on to the user. Thus, the proxy answered the content server's need for information that the content server had requested from the user, thereby avoiding the need for the user to

provide the information and also avoiding the need for a pre-configured entry in the access provider's database for this particular content provider. An intermediary, such as a proxy, provides a secure as well as easy mechanism for content providers to access information and offer new services without having to update commercial terms of agreement in the form of legal contracts. Therefore, the relationship for exchanging information can be established dynamically and instantly.

Figure 5 is a block diagram of a system in which a content provider communicates with both the access provider via a proxy server and a user. Referring to figure 5, the content provider application 503 prepares a message 506 that includes content 504 for the user 501 and content 505 for an access provider via proxy server 502. The content provider application 503 retrieves contents 504 and 505. The content 504, which the user 501 desires, is placed in the body 508 of message 506. The content 505, which the proxy server 502 desires, is placed in the message header 507 of message 506. When the message 506 is transmitted over the network 500, message 506 becomes message 509, content 507 becomes 510, and content 508 becomes 511. The proxy server 502 intercepts message 509 and retrieves content 510 from the header of message 509. Then the content 511 is provided to user 501. Thus, within the same message, the content provider communicates some information to the user, and some (potentially unrelated) information to the access provider.

Figures 6a and 6b depict a scenario of the communication exchange involving a user, access provider via a proxy server and a content provider for a restaurant (hereinafter referred to as Restaurant content provider) using the piggybacked conversation technique. The scenario is as follows:

- 1) The user 601 sends message A, requesting a menu and a map, to a restaurant that is represented by the restaurant content provider 603;
- 2) The proxy server 602 intercepts message A, which contains the user's request, and forwards message A to the restaurant content provider 603;
- 3) The restaurant content provider determines that to best service this request the restaurant content provider 603 should obtain information about the user 601's location for constructing map/directions. Therefore, the restaurant content provider creates message B in order to request user location from the user 601, inserts an indication that the restaurant content provider 603 needs the location of user 601 into the header of message B and transmits message B over network 600.
- 4) The proxy server 602 intercepts message B, which contains the request from the restaurant content provider 603, examines the header of message B and sees the

request for user 601's location. The proxy server 602 retrieves the user location 604 from within the secure network 600. Optionally, the proxy server 602 may first ask permission from the user 601 or check in a user profile (refer to 406) or a content provider profile (refer to 404) to ensure that the content provider 603 has permission to access the location information 604. Note, the user profile 406 and the content provider profile 404 can be implemented as databases.

5) The proxy server 602 creates message C, inserts the user location 604 information into message C, and provides the user location 604 to the restaurant content provider 603 via message C;

6) The restaurant content provider 603 retrieves the user location information 603 from message C. Now that the restaurant content provider 603 has received the user location 604 information, the restaurant content provider 603 generates a map/directions 605 for the user and retrieves the menu 606;

7) The restaurant content provider 603 creates message D, which contains the menu 606, map/directions 605, and transmits provides message D over the network.

8) The proxy server 602 intercepts message D and does the following with message D:

- a) examines the header of message D;
- b) sees there is nothing pertinent in the header of message D; and
- c) forwards message D to user 601.

Optionally, the access provider may also create a content provider profile for the content provider, and indicate within the profile that the content provider desires location information. By inspecting content provider profile, the access provider knows that the service provided by the content provider requires location information. Using this knowledge, the access provider can then proactively insert location information into any subsequent messages that its users send to that content provider, without the content server having to request the location information.

Figure 7 depicts a scenario that is similar to figures 6a and 6b except that the proxy server 702 checks a content provider profile 705 for policy information from the content provider application 703 before forwarding the user 701's request to the content provider application 703. As depicted in figure 7, the user 701 sends a request for information from the restaurant content provider 703 via message 706. When the proxy server 702 intercepts message 706, the proxy server 702 checks the content provider profile 705 and sees that the content provider profile 705 indicates that the user location 704, which is the location of user 701, should be inserted into messages before

forwarding the messages to the restaurant content provider 703. Therefore, the proxy server 702 retrieves the user location 704 and inserts the user location 704 into the header of message 706 and forwards the message 706, which includes the inserted user location, to the restaurant content provider 703. When the restaurant content provider 703 receives the message, the restaurant content provider 703 retrieves the user location" from the header of message 708.

ALTERNATIVES

There is no limit to the type of content that can be transmitted in the piggybacked conversations described above. For example, one participant in the conversation may insert JAVA code into the header for the other participant to execute. Similarly, the inserted data may include multimedia, such a digital video, images, or sound clips. Since the piggybacked conversation takes place transparent to the user, the contents of the piggybacked conversation are typically not presented to the user. Thus, the proxy server may delete the additional information from the headers of messages received from content providers prior to delivering the messages to the users.

In the description given above, the conversation between the proxy server and the third party is piggybacked on the conversation between the user and the third party using the header of the user's messages. However, in alternative embodiments, the conversation is piggybacked by inserting information into portions of the messages other than the header. Within the HTTP context, inserting the data into the header is preferred because recipients and intermediaries that do not have support for such piggybacked conversations simply ignore the inserted fields in the header without causing errors. An example of inserting fields into content is using user invisible fields in HTML, such as the Abstract field. Information can be inserted into invisible fields in the message header or invisible fields on the content or data portion of the message. The proxy server is an intermediary that enables network intelligence to be added to requests and responses without having to extensively change the software infrastructure between the client and the server.

HARDWARE OVERVIEW

Figure 8 is a block diagram that illustrates a computer system 800 upon which an embodiment of the invention may be implemented. Computer system 800 includes a bus 802 or other communication mechanism for communicating information, and a processor 804 coupled with bus 802 for processing information. Computer system 800 also includes

a main memory 806, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 802 for storing information and instructions to be executed by processor 804. Main memory 806 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 804. Computer system 800 further includes a read only memory (ROM) 808 or other static storage device coupled to bus 802 for storing static information and instructions for processor 804. A storage device 810, such as a magnetic disk or optical disk, is provided and coupled to bus 802 for storing information and instructions.

Computer system 800 may be coupled via bus 802 to a display 812, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device 814, including alphanumeric and other keys, is coupled to bus 802 for communicating information and command selections to processor 804. Another type of user input device is cursor control 816, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 804 and for controlling cursor movement on display 812. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane.

The invention is related to the use of computer system 800 for implementing the techniques described herein. According to one embodiment of the invention, those techniques are performed by computer system 800 in response to processor 804 executing one or more sequences of one or more instructions contained in main memory 806. Such instructions may be read into main memory 806 from another computer-readable medium, such as storage device 810. Execution of the sequences of instructions contained in main memory 806 causes processor 804 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 804 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device 810. Volatile media includes dynamic memory, such as main memory 806. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus 802. Transmission media can also take the form of

acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punchcards, papertape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 804 for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 800 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector can receive the data carried in the infra-red signal and appropriate circuitry can place the data on bus 802. Bus 802 carries the data to main memory 806, from which processor 804 retrieves and executes the instructions. The instructions received by main memory 806 may optionally be stored on storage device 810 either before or after execution by processor 804.

Computer system 800 also includes a communication interface 818 coupled to bus 802. Communication interface 818 provides a two-way data communication coupling to a network link 820 that is connected to a local network 822. For example, communication interface 818 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 818 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 818 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

Network link 820 typically provides data communication through one or more networks to other data devices. For example, network link 820 may provide a connection through local network 822 to a host computer 824 or to data equipment operated by an Internet Service Provider (ISP) 826. ISP 826 in turn provides data communication services through the world wide packet data communication network now commonly referred to as the "Internet" 828. Local network 822 and Internet 828 both use electrical,

electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 820 and through communication interface 818, which carry the digital data to and from computer system 800, are exemplary forms of carrier waves transporting the information.

Computer system 800 can send messages and receive data, including program code, through the network(s), network link 820 and communication interface 818. In the Internet example, a server 830 might transmit a requested code for an application program through Internet 828, ISP 826, local network 822 and communication interface 818.

The received code may be executed by processor 804 as it is received, and/or stored in storage device 810, or other non-volatile storage for later execution. In this manner, computer system 800 may obtain application code in the form of a carrier wave. In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method for communicating electronic information comprising the computer-implemented steps of:
intercepting a message sent from a first participant to a second participant;
selecting additional information to convey to said second participant based on information contained in said message;
modifying said message to create a modified message that includes said additional information; and
retransmitting said modified message for receipt by said second participant.
2. The method for Claim 1 wherein said first participant is one of a service requestor and a service provider and the second participant is the other of the service requestor and the service provider.
3. The method for Claim 2 wherein:
the second participant is a service provider; and
the step of selecting comprises the steps of:
determining a service requested by said first participant based on information contained in said message;
determining what information is required by said service; and
selecting information required by said service as said additional information to convey to said second participant.
4. The method for Claim 3 wherein said information required by said service is information, which is not already present in said message, about said first participant.
5. The method for Claim 3 wherein said information required by said service is a current location of said first participant.
6. The method for Claim 2 wherein the step of selecting additional information to convey includes the steps of:

- locating a profile based on information contained in said message; and
obtaining the additional information based on information contained in said
profile.
7. The method of Claim 6 wherein:
the profile is associated with the first participant; and
the step of locating the profile includes locating the profile based on information
within said message that identifies the first participant.
 8. The method of Claim 6 wherein:
the profile is associated with the second participant; and
the step of locating the profile includes locating the profile based on information
within said message that identifies the second participant.
 9. The method for Claim 6 wherein the profile contains information concerning
where to obtain the additional information.
 10. The method for Claim 6 wherein the profile contains authentication information.
 11. The method for Claim 2 wherein the step of modifying said message further
includes the step of inserting the additional information into a header of the
message.
 12. The method for Claim 11 wherein the step of inserting the additional information
into the header of the message includes the step of inserting the additional
information into one or more invisible fields within the header.
 13. The method for Claim 12 wherein the step of modifying said message further
includes the step of inserting the additional information into a data portion of the
message.
 14. The method for Claim 12 wherein the step of inserting the additional information
into the data portion of the message includes the step of inserting the additional
information into one or more invisible fields in the data portion of the message.

15. The method for Claim 2 wherein the additional information is information about the service requestor.
16. The method for Claim 2 wherein the additional information is information about the service provider.
17. The method for Claim 2 wherein the additional information is a request for a second set of additional information.
18. The method for Claim 2 wherein the additional information is a current location of the first participant.
19. The method for Claim 2 wherein the information contained in said message that is used for selecting said additional information is the destination of the message.
20. The method for Claim 1 further comprising the step of obtaining the additional information from within a private network that is not accessible to said first participant.
21. The method for Claim 1 further comprising the step of obtaining the additional information from within a private network that is not accessible to said second participant.
22. The method for Claim 2 wherein the additional information is code for execution by said second participant.
23. The method for Claim 2 wherein the additional information includes at least one of digital video, images, and sound clips.
24. The method for Claim 2 wherein the additional information is multimedia data.
25. The method for Claim 2 wherein the additional information is billing data.
26. The method for Claim 2 further comprising the computer-implemented step of authenticating the first participant prior to retransmitting said modified message.

27. The method for Claim 26 wherein the step of authenticating includes validating a user ID and password combination.
28. The method for Claim 2 further comprising the computer-implemented step of authenticating the second participant.
29. The method for Claim 28 wherein the step of authenticating further includes the step of determining whether the second participant is an approved partner.
30. The method for Claim 2 further comprising the computer-implemented step of: transmitting as part of a response to a user data that indicates terms of agreement with said service provider.
31. A method for communicating electronic information comprising the computer-implemented steps of:
intercepting, at an intermediary, a message sent by a first participant to a second participant;
at said intermediary, reading piggybacked information from said message, wherein said piggybacked information was inserted into said message for said intermediary by said first participant; and
retransmitting said message for receipt by said second participant.
32. The method for Claim 31 further comprising the step of:
authenticating the first participant with an authentication mechanism.
33. The method for Claim 32 wherein the authentication mechanism is digital certificates.
34. The method for Claim 31 further comprising the steps of:
determining whether the first participant is providing said message to said second participant for a fee;
if the first participant is providing said message to said second participant for a fee, then establishing a secure connection with the first participant; and
authenticating the first participant with an authentication mechanism.

35. The method of Claim 31 wherein:
the method further comprises the step of deleting said piggybacked information from said message to create a modified message; and
the step of retransmitting said message is performed by retransmitting said modified message.
36. The method of Claim 35 wherein:
the step of reading piggybacked information includes reading piggybacked information from a header portion of said message; and
the step of deleting said piggybacked information includes removing said piggybacked information from said header portion of said message.
37. The method of Claim 31 wherein said first participant is a service provider, and
the step of reading said piggybacked information includes reading information about a service that said second participant has requested from said first participant.
38. The method of Claim 37 wherein:
prior to retransmitting said message, the intermediary sends the second participant a request for authorization of payment for said service; and
wherein the step of retransmitting said message to said second participant is performed in response to receiving authorization from said second participant.
39. The method of Claim 37 wherein:
prior to retransmitting said message, the intermediary determines whether the second participant has sufficient funds to pay for said service; and
wherein the step of retransmitting said message to said second participant is performed in response to determining that said second participant has sufficient funds to pay for said service.
40. The method of Claim 37 wherein the piggybacked information indicates a fee for said service.

41. The method of Claim 37 further comprising the step of the intermediary storing information for use in billing said second participant for said service based on said piggybacked information.
42. The method of Claim 31 wherein the step of reading piggybacked information includes reading piggybacked information from a header portion of said message.
43. The method of Claim 31 further comprising the step of the intermediary updating a profile associated with said first participant based on said piggybacked information.
44. The method of Claim 31 further comprising the step of the intermediary updating a profile associated with said second participant based on said piggybacked information.
45. The method of Claim 31 wherein said piggybacked information includes terms of agreement.
46. A method for communicating electronic information comprising the computer-implemented steps of:
intercepting, at an intermediary, a message sent by a first participant to a second participant;
at said intermediary, reading piggybacked information from said message,
wherein said piggybacked information was inserted into said message for said intermediary by said first participant;
determining that the piggybacked information indicates that said first participant requires particular information available to said intermediary;
sending the particular information from the intermediary to said first participant.
47. The method of Claim 46 wherein the step of sending said particular information from said intermediary to said first participant is performed without retransmitting said message to said second participant.

48. The method of Claim 47 further comprising the step of:
receiving, at said intermediary, a second message from said first participant that
was generated by said first participant in response to said particular information;
and
retransmitting said second message to said second participant.
49. The method of Claim 46 wherein said particular information is about said second
participant.
50. The method of Claim 49 wherein said particular information includes
location information about said second participant.
51. A computer-readable medium carrying instructions for communicating electronic
information, the instructions including instructions for performing the steps of:
intercepting a message sent from a first participant to a second participant;
selecting additional information to convey to said second participant based on
information contained in said message;
modifying said message to create a modified message that includes said additional
information; and
retransmitting said modified message for receipt by said second participant.
52. The computer-readable medium for Claim 51 wherein said first participant is
one of a service requestor and a service provider and the second participant is
the other of the service requestor and the service provider.
53. The computer-readable medium for Claim 52 wherein:
the second participant is a service provider; and
the step of selecting comprises the steps of:
determining a service requested by said first participant based on
information contained in said message;
determining what information is required by said service; and
selecting information required by said service as said additional
information to convey to said second participant.

54. The computer-readable medium for Claim 53 wherein said information required by said service is information, which is not already present in said message, about said first participant.
55. The computer-readable medium for Claim 53 wherein said information required by said service is a current location of said first participant.
56. The computer-readable medium for Claim 52 wherein the step of selecting additional information to convey includes the steps of:
locating a profile based on information contained in said message; and
obtaining the additional information based on information contained in said profile.
57. The computer-readable medium of Claim 56 wherein:
the profile is associated with the first participant; and
the step of locating the profile includes locating the profile based on information within said message that identifies the first participant.
58. The computer-readable medium of Claim 56 wherein:
the profile is associated with the second participant; and
the step of locating the profile includes locating the profile based on information within said message that identifies the second participant.
59. The computer-readable medium for Claim 56 wherein the profile contains information concerning where to obtain the additional information.
60. The computer-readable medium for Claim 56 wherein the profile contains authentication information.
61. The computer-readable medium for Claim 52 wherein the step of modifying said message further includes the step of inserting the additional information into a header of the message.

62. The computer-readable medium for Claim 61 wherein the step of inserting the additional information into the header of the message includes the step of inserting the additional information into one or more invisible fields within the header.
63. The computer-readable medium for Claim 62 wherein the step of modifying the message further includes the step of inserting the additional information into a data portion of the message.
64. The computer-readable medium for Claim 62 wherein the step of inserting the additional information into the data portion of the message includes the step of inserting the additional information into one or more invisible fields in the data portion of the message.
65. The computer-readable medium for Claim 52 wherein the additional information is information about the service requestor.
66. The computer-readable medium for Claim 52 wherein the additional information is information about the service provider.
67. The computer-readable medium for Claim 52 wherein the additional information is a request for a second set of additional information.
68. The computer-readable medium for Claim 52 wherein the additional information is a current location of the first participant.
69. The computer-readable medium for Claim 52 wherein the information contained in said message that is used for selecting said additional information is the destination of the message.
70. The computer-readable medium for Claim 51 further comprising the step of obtaining the additional information from within a private network that is not accessible to said first participant.

71. The computer-readable medium for Claim 51 further comprising the step of obtaining the additional information from within a private network that is not accessible to said second participant.
72. The computer-readable medium for Claim 52 wherein the additional information is code for execution by said second participant.
73. The computer-readable medium for Claim 52 wherein the additional information includes at least one of digital video, images, and sound clips.
74. The computer-readable medium for Claim 52 wherein the additional information is multimedia data.
75. The computer-readable medium for Claim 52 wherein the additional information is billing data.
76. The computer-readable medium for Claim 52 further comprising the computer-implemented step of authenticating the first participant prior to retransmitting said modified message.
77. The computer-readable medium for Claim 76 wherein the step of authenticating includes validating a user ID and password combination.
78. The computer-readable medium for Claim 52 further comprising the computer-implemented step of authenticating the second participant.
79. The computer-readable medium for Claim 78 wherein the step of authenticating further includes the step of determining whether the second participant is an approved partner.
80. The computer-readable medium for Claim 52 further comprising the computer-implemented step of:
transmitting as part of a response to a user data that indicates terms of agreement with said service provider.

81. A computer-readable medium for communicating electronic information comprising the computer-implemented steps of:
intercepting, at an intermediary, a message sent by a first participant to a second participant;
at said intermediary, reading piggybacked information from said message, wherein said piggybacked information was inserted into said message for said intermediary by said first participant; and
retransmitting said message for receipt by said second participant.
82. The computer-readable medium for Claim 81 further comprising the steps of:
authenticating the first participant with an authentication mechanism.
83. The computer-readable medium for Claim 82 wherein the authentication mechanism is digital certificates.
84. The computer-readable medium for Claim 81 further comprising the steps of:
determining whether the first participant is providing said message to said second participant for a fee;
if the first participant is providing said message to said second participant for a fee, then
establishing a secure connection with the first participant; and
authenticating the first participant with an authentication mechanism.
85. The computer-readable medium of Claim 81 wherein:
the instructions include instructions for performing the step of deleting said piggybacked information from said message to create a modified message; and
the step of retransmitting said message is performed by retransmitting said modified message.
86. The computer-readable medium of Claim 85 wherein:
the step of reading piggybacked information includes reading piggybacked information from a header portion of said message; and
the step of deleting said piggybacked information includes removing said piggybacked information from said header portion of said message.

87. The computer-readable medium of Claim 81 wherein said first participant is a service provider, and the step of reading said piggybacked information includes reading information about a service that said second participant has requested from said first participant.
88. The computer-readable medium of Claim 87 wherein:
prior to retransmitting said message, the intermediary sends the second participant a request for authorization of payment for said service; and
wherein the step of retransmitting said message to said second participant is performed in response to receiving authorization from said second participant.
89. The computer-readable medium of Claim 87 wherein:
prior to retransmitting said message, the intermediary determines whether the second participant has sufficient funds to pay for said service; and
wherein the step of retransmitting said message to said second participant is performed in response to determining that said second participant has sufficient funds to pay for said service.
90. The computer-readable medium of Claim 87 wherein the piggybacked information indicates a fee for said service.
91. The computer-readable medium of Claim 87 further comprising the step of the intermediary storing information for use in billing said second participant for said service based on said piggybacked information.
92. The computer-readable medium of Claim 81 wherein the step of reading piggybacked information includes reading piggybacked information from a header portion of said message.
93. The computer-readable medium of Claim 81 further comprising the step of the intermediary updating a profile associated with said first participant based on said piggybacked information.

94. The computer-readable medium of Claim 81 further comprising the step of the intermediary updating a profile associated with said second participant based on said piggybacked information.
95. The computer-readable medium of Claim 81 wherein said piggybacked information includes terms of agreement.
96. A computer-readable medium for communicating electronic information comprising the computer-implemented steps of:
intercepting, at an intermediary, a message sent by a first participant to a second participant;
at said intermediary, reading piggybacked information from said message, wherein said piggybacked information was inserted into said message for said intermediary by said first participant;
determining that the piggybacked information indicates that said first participant requires particular information available to said intermediary;
sending the particular information from the intermediary to said first participant.
97. The computer-readable medium of Claim 96 wherein the step of sending said particular information from said intermediary to said first participant is performed without retransmitting said message to said second participant.
98. The computer-readable medium of Claim 97 further comprising the step of:
receiving, at said intermediary, a second message from said first participant that was generated by said first participant in response to said particular information;
and
retransmitting said second message to said second participant.
99. The computer-readable medium of Claim 96 wherein said particular information is about said second participant.
100. The computer-readable medium of Claim 99 wherein said particular information includes location information about said second participant.

101. A system comprising:
a first participant;
a second participant;
an intermediary communicatively coupled between said first participant and said second participant through which messages between said first participant and said participant pass;
the intermediary being configured to communicate information to said second participant by piggybacking information for said second participant onto messages sent to said second participant from said first participant; and
the second participant being configured to communicate information to said intermediary by piggybacking information for said intermediary onto messages sent to said first participant from said second participant.
102. The system of Claim 101 wherein the intermediary resides in a secure network that contains information to which the second participant does not have access, and wherein at least some of the piggybacked information sent from the intermediary to the second participant includes information from within said secure network.

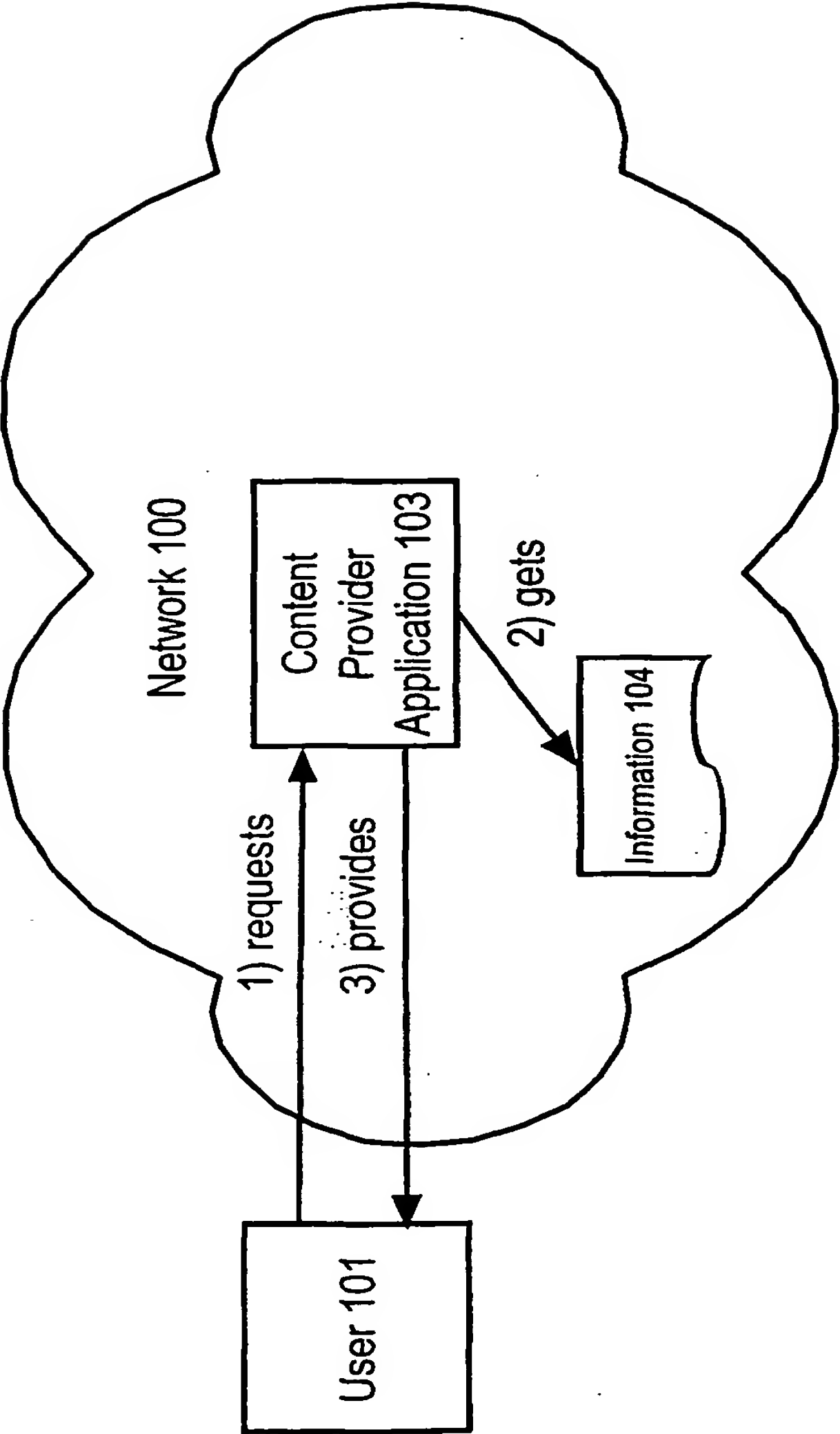


Fig. 1

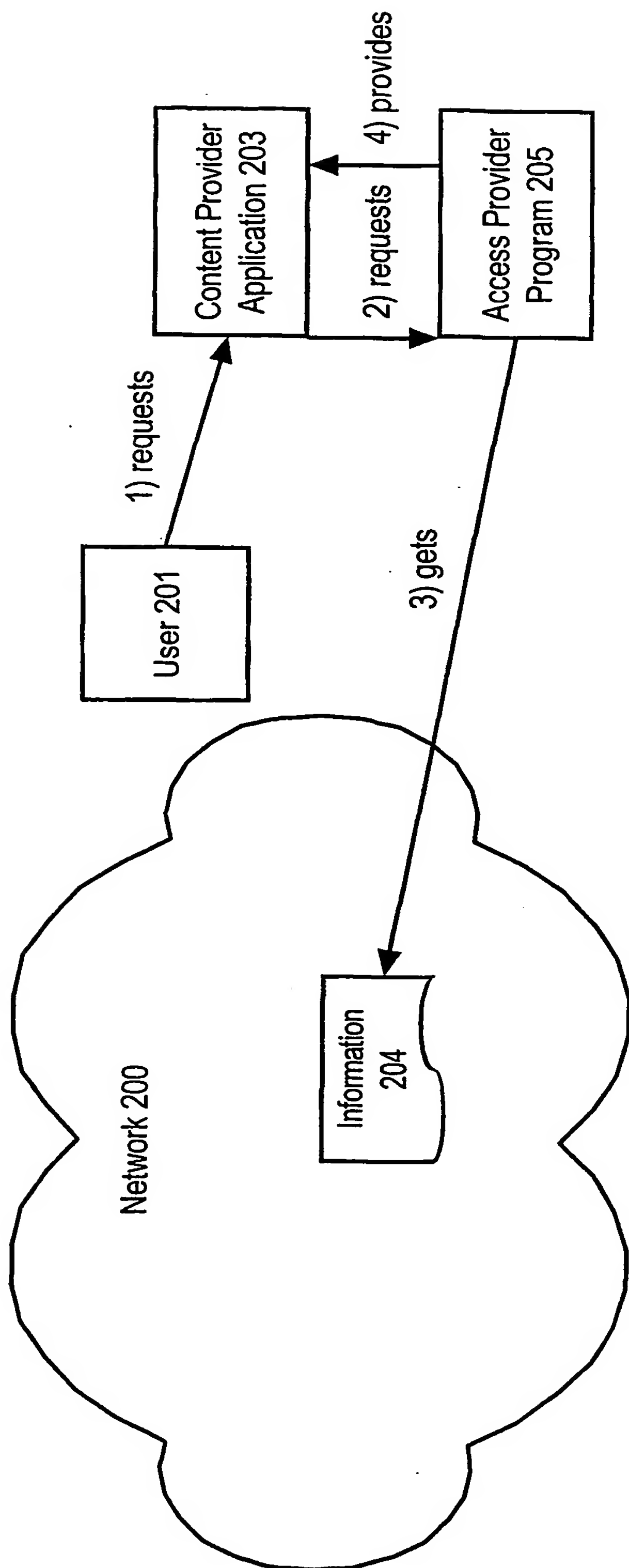


Fig. 2

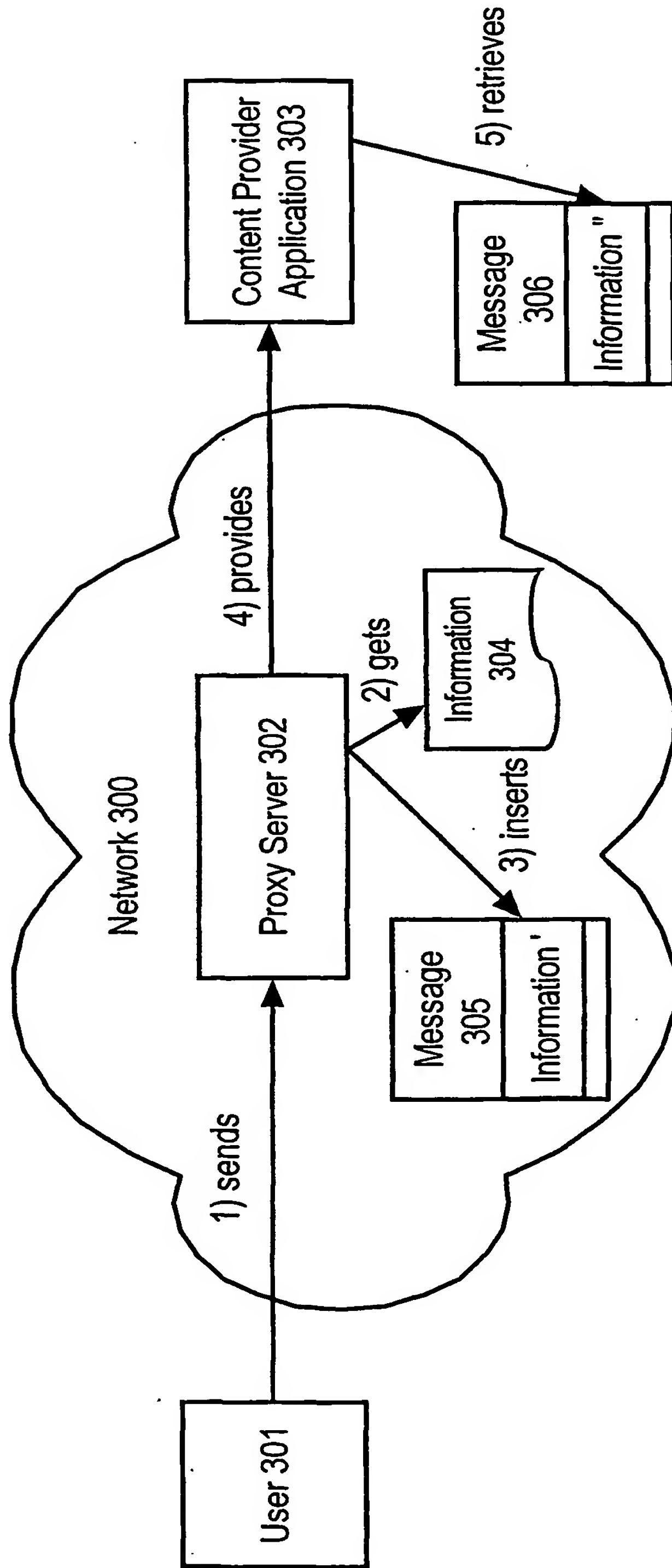


Fig. 3

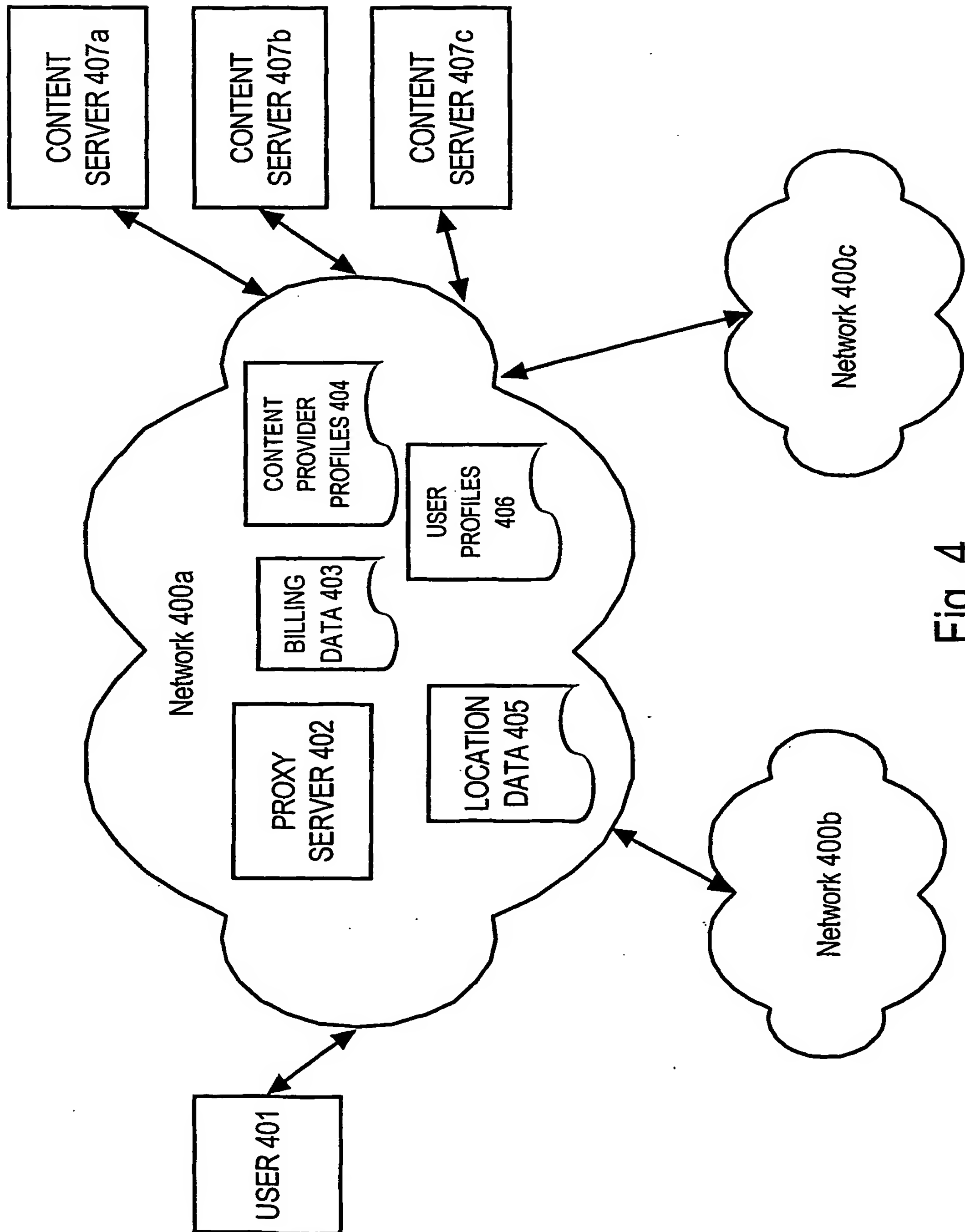


Fig. 4

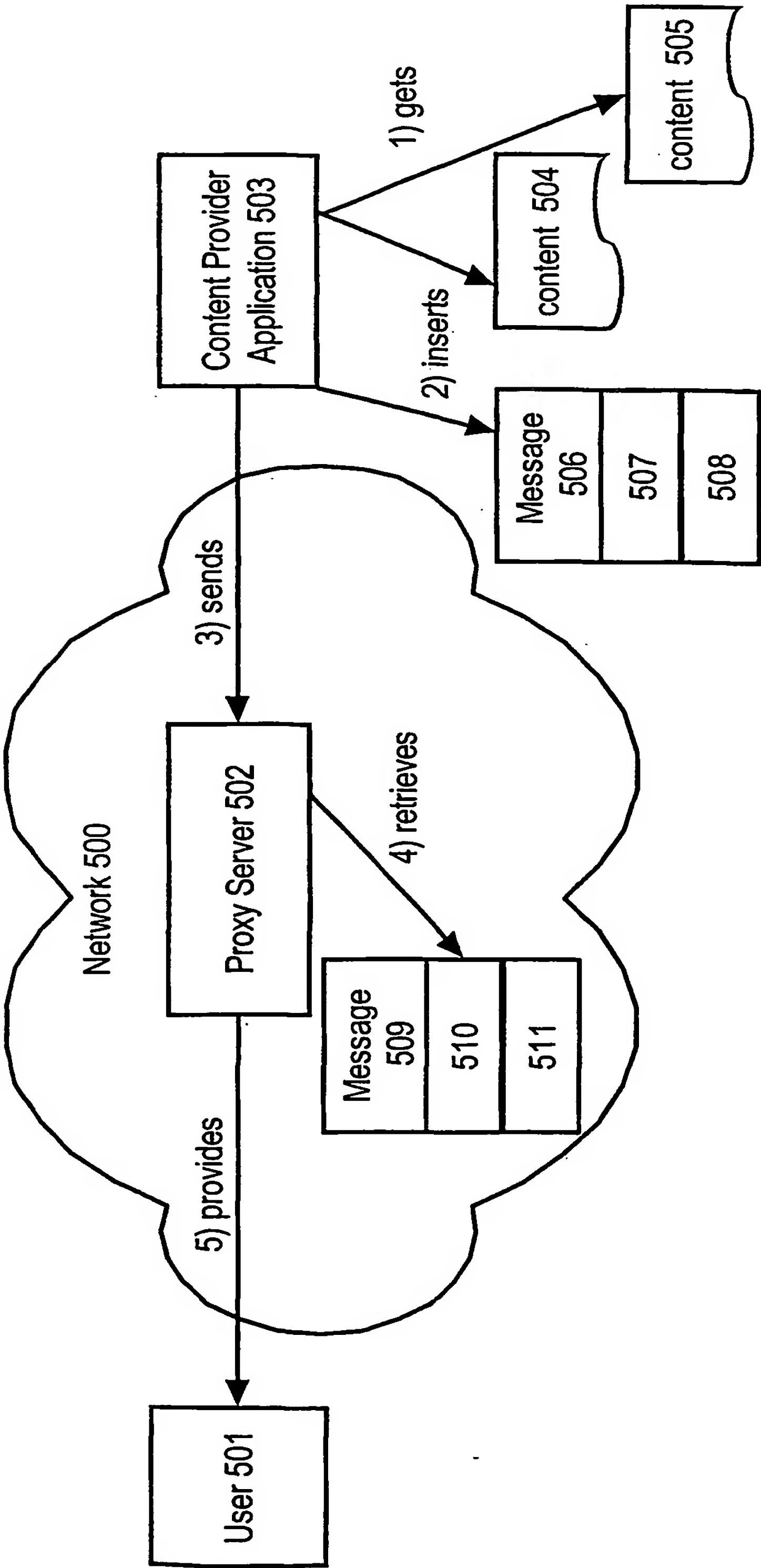


Fig. 5

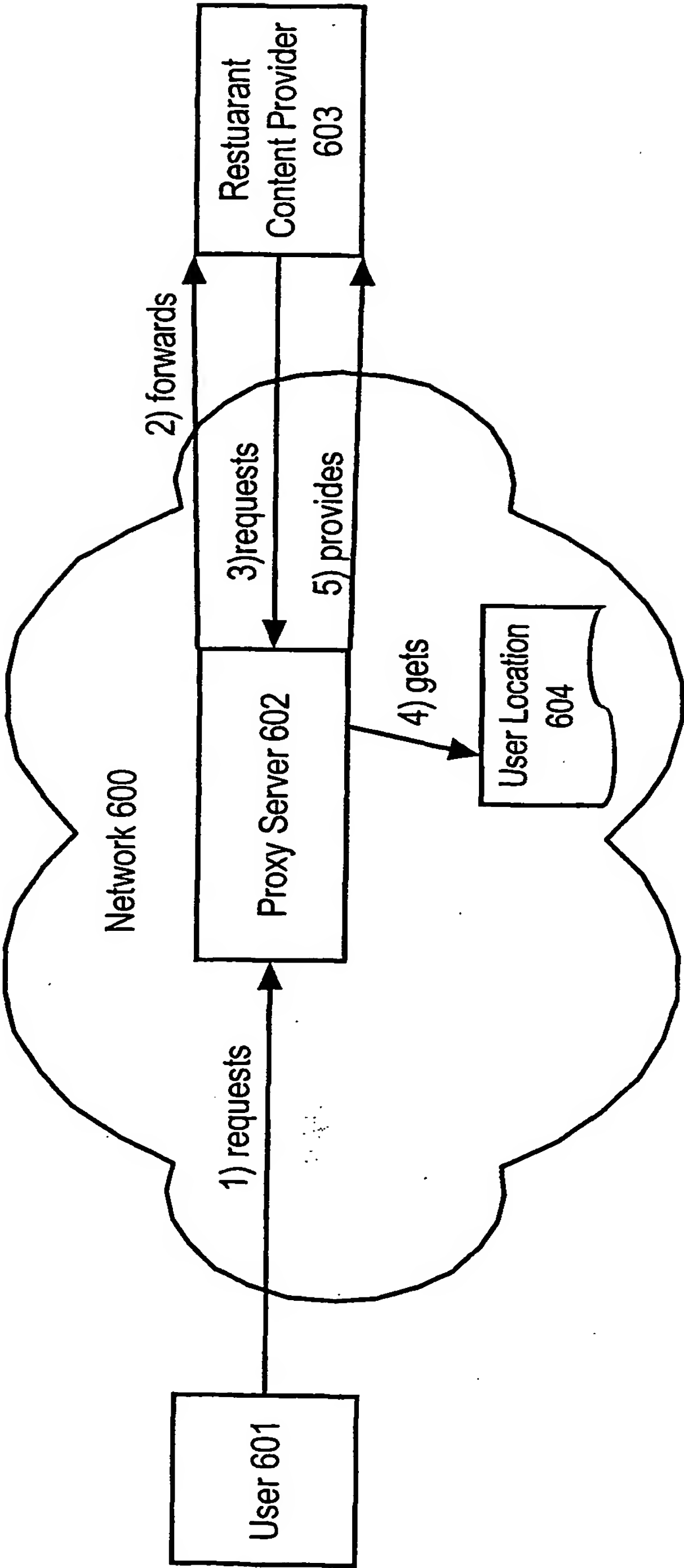


Fig.6a

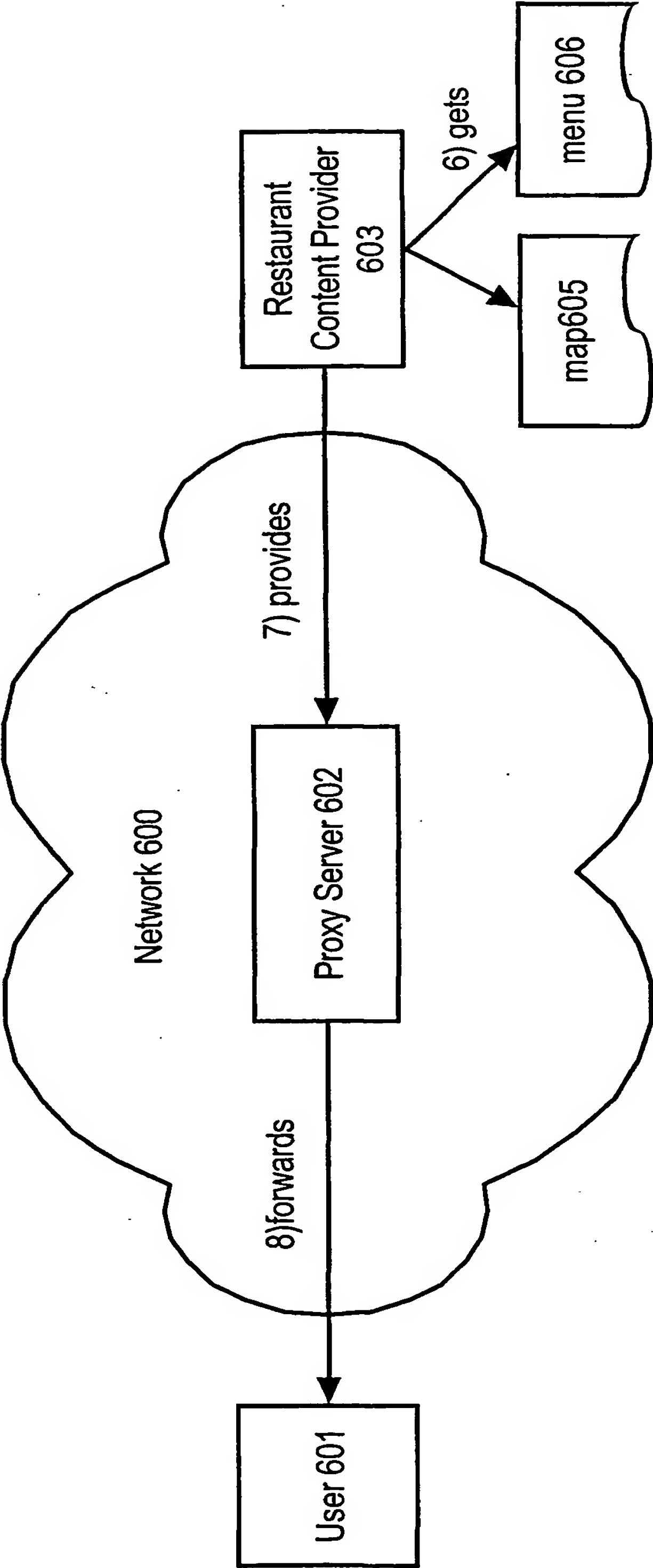


Fig.6b

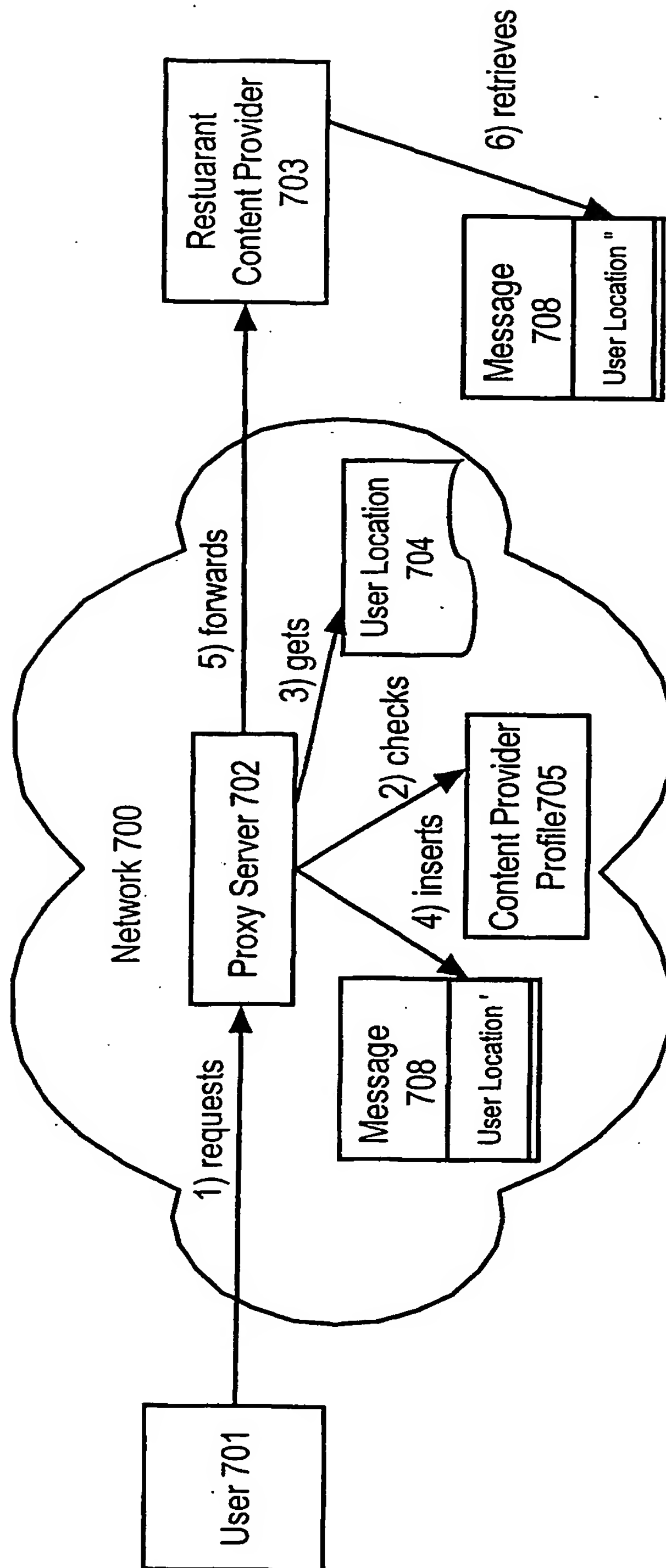
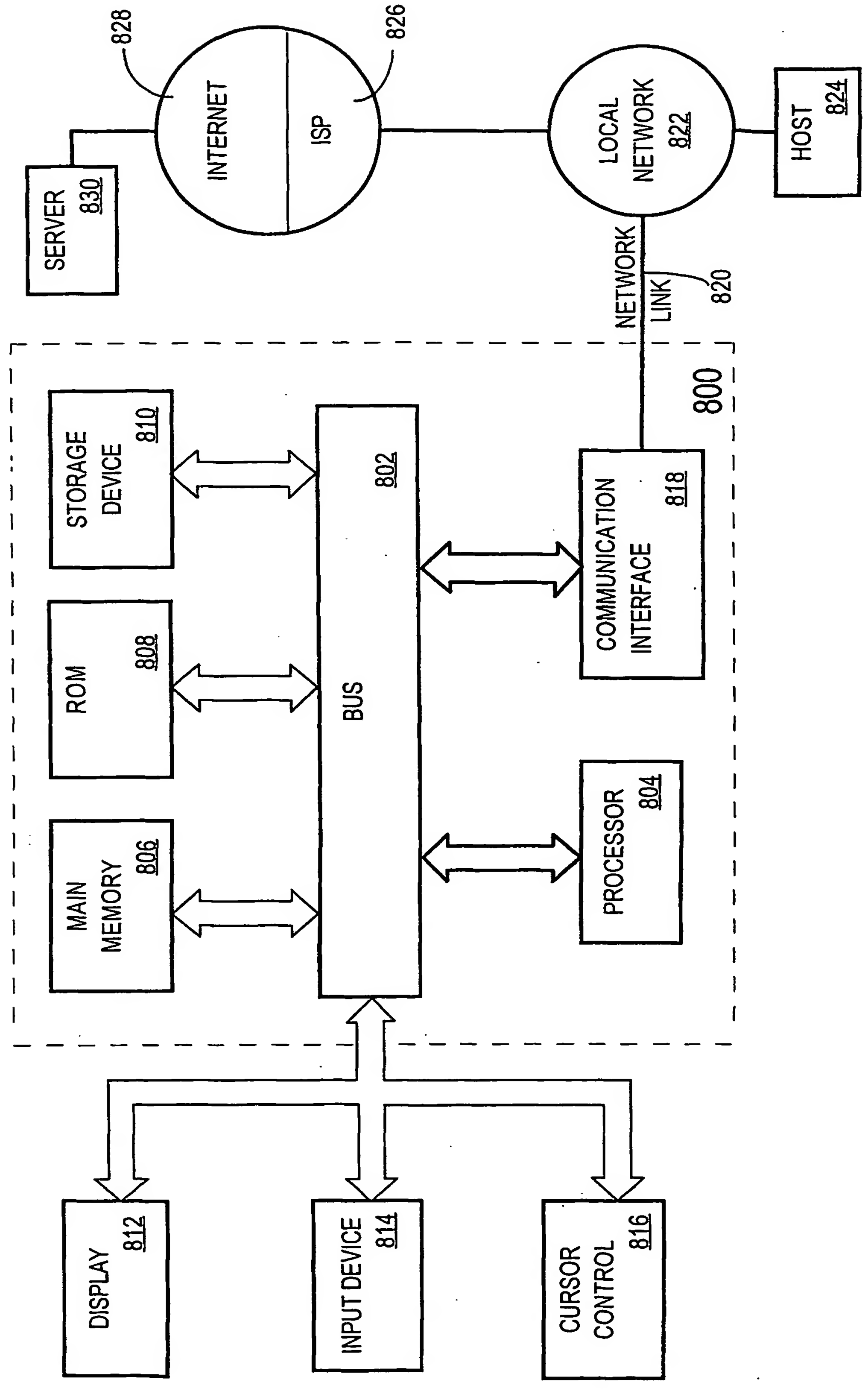


Fig. 7

FIG. 8



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067544 A3

(51) International Patent Classification⁷: **H04L 29/06**

(21) International Application Number: PCT/US02/04641

(22) International Filing Date: 15 February 2002 (15.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/269,699 17 February 2001 (17.02.2001) US

(71) Applicant: **INKTOMI CORPORATION** [US/US]; 4100
East Third Avenue, Foster City, CA 94404 (US).

(72) Inventor: **TSO, Michael**; 20555 Ashley Way, Saratoga,
CA 95070 (US).

(74) Agents: **EICHSTAEDT, Cheryl et al.**; Hickman Palermo
Truong & Becker, LLP, 1600 Willow Street, San Jose, CA
95125 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN,
YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,
GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG).

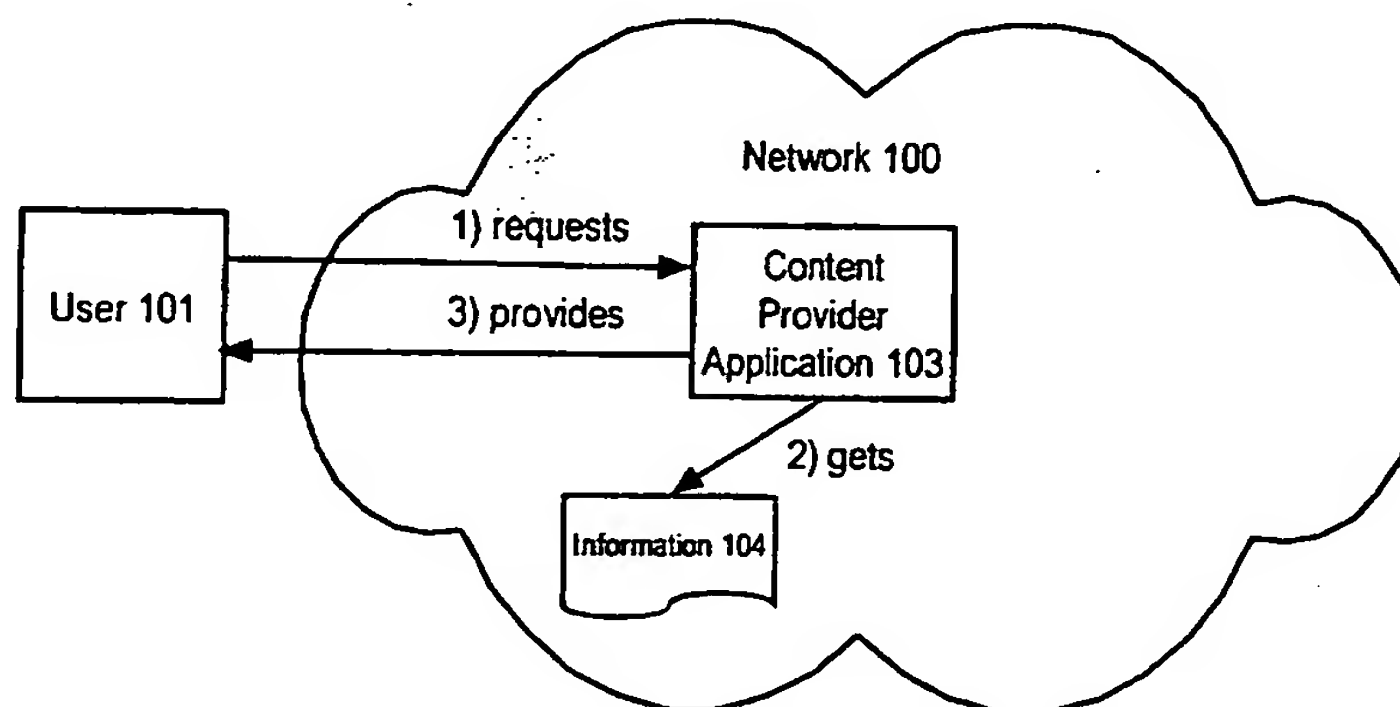
Published:

— with international search report

(88) Date of publication of the international search report:
6 November 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **HEADER-BASED NETWORK API**



(57) Abstract: A method and apparatus for communicating with entities outside of a secure network by intercepting and modifying messages is provided. Techniques for accomplishing the communication include inserting, retrieving, and deleting information from messages. The entities involved in the communication include, but are not limited to, users, content providers, and access providers. Furthermore, the types of information used in modifying messages include billing, location, demographic information, profile data, multimedia data, and code.

WO 02/067544 A3

INTERNATIONAL SEARCH REPORT

Inter nal Application No

PCT7US 02/04641

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 00471 A (DOGON GIL ;KRAMER SHLOMO (IL); SHWED GIL (IL); ZUK NIR (IL); BEN R) 3 January 1997 (1997-01-03) page 4; claim 1	1-30, 51-80
A	EP 0 511 926 A (IBM) 4 November 1992 (1992-11-04) claim 1	1-30, 51-80



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

11 March 2003

Date of mailing of the international search report

04 07. 2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

VEEN, G

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 02/04641

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-30, 51-80

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-30,51-80

Intercepting a message, adding information to it and retransmitting it

2. Claims: 31-45,81-95

Intercepting a message, reading piggybacked information from it and forwarding the message to the destination.

3. Claims: 46-50,96-100

Intercepting a message, reading piggybacked information from it and sending particular information to the source if so indicated by said piggybacked information

4. Claims: 101,102

Transferring messages via an intermediary, the intermediary and the message destination communicating using piggybacked information

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No

PCT/US 02/04641

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 9700471	A	03-01-1997	US	5606668 A		25-02-1997
			AU	6135696 A		15-01-1997
			CA	2197548 A1		03-01-1997
			EP	0807347 A2		19-11-1997
			WO	9700471 A2		03-01-1997
			JP	10504168 T		14-04-1998
			NO	970611 A		15-04-1997
			US	5835726 A		10-11-1998
			CA	2138058 A1		16-06-1995
			DE	69425038 D1		03-08-2000
			DE	69425038 T2		08-03-2001
			EP	0658837 A2		21-06-1995
			JP	8044642 A		16-02-1996
			EP 0511926	A	04-11-1992	US
DE	69211418 D1					18-07-1996
DE	69211418 T2					05-12-1996
EP	0511926 A1					04-11-1992
JP	2093310 C					18-09-1996
JP	5102972 A					23-04-1993
JP	8010863 B					31-01-1996